Robert Mackey, Esq. (SBN 125961)
bobmackeyesq@aol.com
LAW OFFICES OF ROBERT MACKEY
660 Baker Street
Building A, Suite 201
Costa Mesa, CA 92626
Tel. (412) 370-9110
(Additional counsel listed on signature page)

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

BRUCE RIGGS, individually and on behalf of all others similarly situated, *Plaintiff,* *vs.* *TRISTAR INSURANCE GROUP, Inc.* *Defendant.*	CASE NO.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

1. Plaintiff Bruce Riggs ("Plaintiff" or "Plaintiff Riggs") individually and on behalf of all others similarly situated, through his undersigned counsel, hereby alleges the following against Defendant TRISTAR INSURANCE GROUP, Inc. ("TRISTAR" or "Defendant").

2. Plaintiff brings this class action on behalf of all persons whose names, Social Security numbers, and payment card information (collectively known as "personally identifiable information" or "PII") were compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents.

3. Defendant provided insurance program management administration services for Plaintiff and Class Members.

4. However, on November 10, 2022, Defendant discovered unusual activity on its computer systems. A subsequent investigation showed that an unauthorized user had accessed TRISTAR's email system on November 4, 2022, and the personally identifiable information of its customers via "certain TRISTAR systems" on November 9, 2022 (hereinafter "Data Breach"). Upon information and belief, the PII of thousands of individuals was compromised.

5. Defendant's security failures enabled the hackers to steal the personally identifiable information of Plaintiff and members of the Class (defined below). These failures put Plaintiff's and Class Members' PII and interests at serious, immediate, and ongoing risk. Additionally, the Data Breach resulted in costs and expenses to Plaintiff and Class Members associated with time spent and the loss of productivity from addressing and attempting to ameliorate and mitigate the actual and future consequences of the Data Breach, including, as appropriate: reviewing records for fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of

dealing with the consequences of TRISTAR's data security failures.

6. Defendant did not send affected individuals breach notification letters until February 1, 2024. Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach for nearly fifteen (15) months left them particularly vulnerable to having their PII misused.

7. Plaintiff and Class Members have already experienced unauthorized use of their compromised PII, including fraudulent charges to their payment cards.

8. Thus, Plaintiff and Class Members have suffered ascertainable losses in the form of actual fraudulent misuse of their compromised personally identifiable information, out-of-pocket expenses dealing with and mitigating the direct impact of the Data Breach on their lives, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

9. The Data Breach was caused and enabled by Defendant's violation of its obligations to abide by best practices, industry standards, and federal and state laws concerning the security of individuals' PII. Defendant knew or should have known that its failure to take reasonable security measures—which could have prevented or mitigated the Data Breach that occurred—left its customers' personally identifiable information vulnerable to identity theft, financial loss, and other associated harms.

10. Defendant and its employees failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored its network and/or systems, it would have discovered the Data Breach sooner.

11. The potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the customers' personally identifiable information from those risks left that property exposed.

12. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct.

13. Accordingly, Plaintiff asserts claims for negligence, breach of implied contract,

unjust enrichment/quasi-contract, breach of confidence, and violation of the Oklahoma Consumer Protection Act, Okla. Stat. tit. 15, § 751, et. seq.

14. Plaintiff also seeks injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

PARTIES

A. PLAINTIFF BRUCE RIGGS

15. Plaintiff Bruce Riggs ("Plaintiff" or "Plaintiff Riggs") is, and all times mentioned herein was, an adult resident and citizen of Oklahoma. Plaintiff is a former employee of ADDvantage Technologies Group (hereinafter "ADDvantage"). ADDvantage utilized TRISTAR's insurance program management services. Therefore, Plaintiff has suffered and will continue to suffer injuries and damages as set forth below.

16. Plaintiff brings this action in his individual capacity and on behalf of all others similarly situated.

17. While an ADDvantage employee, Mr. Riggs had a flexible spending insurance plan that was managed by TRISTAR. This is how TRISTAR obtained Mr. Riggs' personally identifiable information.

18. On or around February 12, 2024, Plaintiff received a letter from TRISTAR dated February 1, 2024, notifying him of the Data Breach related to his insurance plan while employed at ADDvantage.

19. Plaintiff Riggs has suffered, and continues to suffer from, actual and imminent identity theft and misuse of his PII as a direct and/or proximate result of TRISTAR's actions and inactions.

20. Subsequent to the Data Breach, and in addition to the injuries and damages alleged herein, on or around June of 2023, Plaintiff was notified of unauthorized activity on his debit card. Plaintiff has disputed this charge and undertaken recommended steps to address this unlawful activity. Hence, Plaintiff Riggs has spent a considerable amount of time combatting this fraud. This activity has caused Plaintiff a significant amount of anxiety, and he is deeply worried

about his identity being stolen because of the Data Breach.

21. TRISTAR's conduct, which allowed the Data Breach to occur, caused Plaintiff Riggs significant injuries and harm, including but not limited to, the following: Plaintiff devoted (and must continue to devote) time, energy, and money to closely monitoring his medical statements, bills, records, and credit and financial accounts; changing login and password information on any sensitive account even more frequently than he already does; and screening and scrutinizing phone calls, emails, and communications more carefully to ensure that he is not being targeted on a social engineering or spear phishing attack. Plaintiff has taken or will be forced to take these measures to mitigate his potential damages that are fairly traceable to the Data Breach.

22. Once PII is exposed, there is virtually no way to ensure that the compromised information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff will need to maintain these heightened measures for years, and possibly his entire life.

23. Plaintiff is also at a continued imminent and substantial risk of harm because his PII remains in TRISTAR's systems, which have already proven susceptible to compromise and attack, and are subject to an increased and imminent future attack.

24. As a result of the Data Breach, and in addition to the time Plaintiff Riggs has spent and anticipates spending to mitigate the impact of the Data Breach on his life, Plaintiff also suffered emotional distress from the public release of his PII that he believed would be protected from unauthorized access and disclosure. The emotional distress he experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing his PII for identity theft and fraud.

25. Additionally, Plaintiff has suffered damage to and diminution in the value of his highly sensitive and confidential PII, a form of property that Plaintiff provided and entrusted to TRISTAR, and which was compromised because of the Data Breach TRISTAR failed to prevent. Plaintiff has also suffered a violation of his privacy rights caused by the unauthorized disclosure of his PII.

26. The free credit monitoring and identity restoration services offered by TRISTAR after the Data Breach were and continue to be ineffective because these services would require the sharing of Plaintiff Riggs' sensitive information with third parties, and TRISTAR cannot guarantee complete privacy thereof.

27. Moreover, the time Plaintiff spent dealing with these incidents resulting from the Data Breach is time he would have spent on other life activities. In addition, the time Plaintiff lost was spent at TRISTAR's direction. Indeed, in the notice letter Plaintiff received, TRISTAR directed Plaintiff to review his accounts and credit reports for unauthorized activity.

28. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details of the incident.

29. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

B. DEFENDANT

68. Defendant TRISTAR Insurance Group has its principal place of business at 100 Oceangate, Suite 840 Long Beach, CA 90802. TRISTAR's corporate policies, including those on data privacy, are established in and emanate from the State of California.

JURISDICTION AND VENUE

69. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Defendant's citizenship, including Plaintiff Riggs, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

70. The Court has personal jurisdiction over Defendant because its principal place of business is located, and it conducts substantial business, in this District.

71. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant

maintains its principal place of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant's Business and The Data Breach

72. Plaintiff and Class Members were either employees or customers of TRISTAR's subsidiaries. Specifically, TRISTAR provided insurance administration services to various entities, including ADDvantage. Consequently, Defendant routinely collects sensitive personal data including names, Social Security numbers (ssn), and payment card information.

73. In or around early February 1, 2024, Defendant issued a Notice Letter to Plaintiff and Class Members, alerting them that their sensitive personally identifiable information had been exposed in a Data Breach. Below is a section of the aforementioned letter:

WHAT HAPPENED? On or about November 10, 2022, TRISTAR became aware of suspicious activity on certain computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to our email environment beginning on November 4, 2022, and that the unauthorized actor was ultimately able to gain access to certain TRISTAR systems beginning on November 9, 2022. Through our investigation, we learned that certain information related to our customers was potentially exfiltrated from TRISTAR's network. TRISTAR therefore undertook a comprehensive and time intensive review of potentially impacted files, with the assistance of third-party subject matter specialists, and later determined that the files contained certain information related to you. TRISTAR has seen no evidence of misuse of any information related to this event. Additionally, there is no evidence that TRISTAR or ADD VANTAGE TECHNOLOGIES GROUP's claims or accounting systems were breached during this incident.

WHAT INFORMATION WAS INVOLVED? TRISTAR determined that the following

information related to you was present within the impacted files: your name, SSN.

74. Based on the Notice Letter sent to Plaintiff and Class Members, Defendant was alerted to unusual activity indicating unauthorized access to its computer systems on November 10, 2022. Particularly, the unauthorized user accessed customers' PII via TRISTAR's systems on November 9, 2022.

75. The delay between the initial discovery of the Data Breach and the notification to affected customers caused Plaintiff and Class Members harm they otherwise could have avoided had a timely disclosure been made.

76. Omitted from the Notice Letter was any explanation as to why Defendant failed to provide the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such breaches do not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their personally identifiable information remains protected.

77. Thus, this "disclosure" amounts to no real disclosure at all, as it fails to inform (with any degree of specificity) Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the hacking is severely diminished.

78. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it maintains for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed.

79. The Notice Letter also offered twelve (12) months of free credit monitoring and identity theft restoration services, as well as generic information regarding steps that victims of data security incidents can take to protect their personal information.

80. Defendant's offer to provide twelve (12) months of credit monitoring is woefully inadequate. Credit monitoring only alerts individuals to the misuse of their information after it happens, which might not take place until years after the exposure of their PII.

81. Defendant disregarded the rights of Plaintiff and Class Members by intentionally,

willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' personally identifiable information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data. As a result, the PII of Plaintiff and Class Members was exfiltrated through unauthorized access by an unknown, malicious cyber hacker with the intent to fraudulently misuse it. Plaintiff and Class Members have a continuing interest in ensuring that their compromised Information is and remains safe.

82. If Plaintiff and Class Members knew of TRISTAR's inadequate data security, they would have not entrusted it with their highly sensitive PII.

B. Defendant Failed to Comply with Industry Standards and Federal and State Law

83. In the ordinary course of its business as a third-party insurance claims administrator, TRISTAR requires that its customers, and the customers of its subsidiaries, entrust it with their highly confidential personal information, such as their names, social security numbers, and credit and/or debit card details.

84. At the time of the Data Breach, TRISTAR had a Privacy Notice in place that, upon information and belief, promised its customers that it would only share their PII in limited circumstances and with specific third parties, and that it would safeguard their data. Particularly, TRISTAR's privacy policy[1] states:

> We may share your personal data within TRISTAR's group of companies for the purpose of your interaction with us, such as for the provision of our Services, general business operations, marketing, data analytics, surveys, benchmarking, and compliance with applicable laws.
> We may also share your personal data with the following third parties for the purpose of your interaction with us…..

[1] *See* TRISTAR's Privacy Notice, available at https://www.tristarrisk.com/pdf/Privacy%20Policy.pdf #whoweshareyourdatawith and #howweprotectyourdata (last viewed on February 23, 2024). Though the Privacy Notice was last updated on or about June 2023, it was initially effective as of January 2020. To the extent the current revision is materially different from the Notice in place on January 2020, and was effective during the Data Breach that occurred on November 9, 2022, Plaintiff reserves the right to amend this Complaint.

> We use a range of organizational and technical security measure to protect your personal data, including the following:
>
> - Restricted access to those who need to know for the purposes set out in our underlying agreement or this Privacy Notice. Firewalls to block unauthorized traffic to servers.
> - Physical servers located insecure locations and accessible only by authorized personnel.
> - Internal procedures governing the storage, access, and disclosure of your personal data.
> - Additional safeguards as may be required by applicable laws in the jurisdictions where we process your personal data.

85. By obtaining, collecting, and gathering Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the aforesaid sensitive information from disclosure.

86. Defendant had obligations created by industry standards and federal and state law to keep Class Members' PII confidential and to protect it from unauthorized access and disclosure.

87. Plaintiff and Class Members provided their personally identifiable information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligation to keep such information confidential and secure from unauthorized access.

88. Defendant's failure to provide adequate security measures to safeguard Plaintiff's and Class Members' PII is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' PII.

89. The number of U.S. data breaches surpassed 1,800 in 2021, a record high and a

sixty-eight percent increase in the number of data breaches from the previous year.[2]

90. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breach and cyberattacks have resulted in significant harms to customers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for customers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).[3]

91. Charged with handling sensitive PII, Defendant knew, or should have known, the importance of safeguarding its customers' personally identifiable information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed upon customers after a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

92. Despite the abundance and availability of information regarding cybersecurity best practices for the insurance industry, Defendant chose to ignore them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of customers' PII.

93. At a minimum, industry best practices should have been implemented by an insurance administrator like Defendant, including but not limited to requiring customers to create strong passwords; implementing multi-layer security including firewalls and anti-malware software; encrypting data and making it unreadable without a key; updating and patching all

---

[2] Identity Theft Resource Center, *2021 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

[3] CONSUMER FIN. PROT. BUREAU, *Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information* (Aug. 11, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf.

systems with the latest security software; and better educating its employees about safe data security practices.

94. Defendant apparently did not follow these precautions because cybercriminals accessed customers' PII from its systems in November 2022.

95. Defendant was also on notice that under the FTC Act, Defendant is prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for customers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[4]

96. Defendant is further required by the comprehensive data privacy regimes enacted by at least 12 other states to protect Plaintiff's and Class Members' PII, and further, to handle any breach of the same in accordance with applicable breach notification statutes.[5]

97. The potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take reasonable steps necessary to secure the personally identifiable information from those risks left the impacted parties' PII in a vulnerable position.

C. Defendant Exposed Customers to Identify Theft, Financial Loss, and Other Harms

98. Plaintiff and Class Members have been injured by the disclosure of their PII in the Data Breach.

99. The fact that Plaintiff's and Class Members' PII was stolen means that it is likely for sale by cybercriminals and will be misused in the future.

100. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes

---

[4] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[5] International Association of Privacy Professionals, *Delaware Governor Signs Personal Data Privacy Act* (Sep. 12, 2023), https://iapp.org/news/a/delaware-governor-signs-personal-data-privacy-act.

including identify theft and financial fraud.[6] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground internet websites, commonly referred to as the "dark web."

101. The value of Plaintiff's and Class Members' PII on the black market is substantial. Notably, studies confirm that the average direct financial loss for identity theft victims in 2014 was $1,349.[7]

102. The FTC has also recognized that consumer data is a valuable form of currency. In an FTC roundtable presentation, a former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[8]

103. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[9] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their PII. This business has created a new market for the sale and purchase of this valuable data.

104. The ramifications of Defendant's failure to keep customers' PII secure are long-

---

[6] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[7] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[8] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[9] *Web's Hot New Commodity*, *supra* note 17.

lasting and severe. Once this information is stolen, fraudulent use of the same and damage to victims may continue for years. Furthermore, fraudulent activity might not show up for six to twelve months or even longer.

105. At all relevant times, Defendant was aware, or reasonably should have been aware, that the PII it maintains is highly sensitive and could be used for unlawful purposes by unauthorizes parties (i.e., identity theft and fraud).

106. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the breach of its systems and the theft of customers' personally identifiable information.

107. As mentioned above, the compromised PII in the Data Breach is of great value to cybercriminals and can be used in a variety of malignant ways. Specifically, information about an individual that can be logically connected to other information can be chained together, increasing its utility to criminals and harm to the individuals.

108. Further, as technology advances, computer programs can scan the internet with broader scopes to create a mosaic of data, which may be used to link information to an individual in ways that were not previously feasible. This is known as the "mosaic effect."

109. For example, armed with just a name and date of birth, a data thief can use a hacking technique referred to as "social engineering" to obtain even more information about a victim, such as a person's login credentials. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls, text messages, or phishing emails. A data breach can be the starting point for these additional targeted attacks.

110. One such example of criminals piecing together bits and pieces of compromised

PII for profit is the development of "Fullz" packages.[10]

111. With "Fullz" packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy, as to assemble complete dossiers on individuals.

112. Here, the development of "Fullz" packages means that the stolen PII from the Data Breach can easily be used to link and identify Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. As a result, even if information such as emails and phone numbers are not included in the personally identifiable information that was exfiltrated in the Data Breach, criminals may still create a Fullz package and sell it to other criminals and unscrupulous operators (such as illegal and scam telemarketers) *ad nauseam*.

113. The existence and prevalence of "Fullz" packages means that the PII stolen from the Data Breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and Class Members.

114. Thus, even if certain information, such as Social Security numbers, was not stolen in the Data Breach—which it was, here—criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—

---

[10] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

to crooked operators and other criminals (like illegal and scam telemarketers).

115. In sum, the personally identifiable information exposed here is highly valuable to cybercriminals and can be used in a variety of unlawful ways, to Plaintiff's and Class Members' substantial detriment.

D. Plaintiff and Class Members Suffered Damages from the Data Breach

116. Plaintiff and the Class have been damaged by the compromise of their PII in the Data Breach.

117. The ramifications of Defendant's failure to safeguard customers' personally identifiable information are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[11]

118. In addition to its obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiff and Class Members to protect the PII they entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

119. Defendant further owed and breached its duty to Plaintiff and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

120. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiff's and Class Members' PII. Plaintiff and members of the Class are also at a heightened and increased

---

[11] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

substantial risk of suffering future identity theft and fraud.

121. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some customers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing, or vehicles because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

122. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiff's (and potentially other Class Members') lives. For example, Plaintiff received a cryptically written Notice Letter from Defendant stating that their personally identifiable information was compromised, and that they should remain vigilant for fraudulent activity, with no other explanation of where this information could have gone, or who might have access to it. This has Plaintiff, and likely the other Class Members, riddled with stress and anxiety.

123. Plaintiff and the Class face a substantial risk of suffering out-of-pocket losses, such as unauthorized charges on online accounts, credit card fraud, applications for benefits made in their names, unauthorized loan applications, unaffiliated medical services billed to them, government benefits fraudulently drawn in their name, and other forms of identity theft. Some Class Members have already been victims of identity theft and fraud, as alleged herein.

124. Plaintiff and Class Members have, may have, and/or will have incurred out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, and similar costs directly or indirectly related to the Data Breach.

125. Plaintiffs and Class Members would not have consented to receiving services from TRISTAR had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and/or did not have proper data security practices to safeguard their personally identifiable information from criminal theft and misuse.

126. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

127. Plaintiffs and Class Members now face a real and continuing immediate risk of identity theft and other issues specifically associated with the disclosure of their Social Security numbers, and will need to monitor their credit for an indefinite duration. For Plaintiff and Class Members, this risk creates unending feelings of fear and anxiety.

128. As a result of the Data Breach, Plaintiff's and Class Members' PII has diminished in value.

129. The personally identifiable information belonging to Plaintiff and Class Members is private and was left inadequately protected by Defendant (who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person pursuant to applicable law and industry standards). As a direct result of its inadequate security measures, Defendant disclosed Plaintiff's and Class Members' PII.

130. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' personally identifiable information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

131. Defendant had the resources and the foreknowledge necessary to prevent the Data Breach. However, it neglected to adequately implement data security measures, despite its obligation to protect customer data.

132. Defendant did not properly train its employees, particularly its information technology department, to timely identify cyber-attacks and other data security risks.

133. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class Members' PII.

134. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing

increased risk of harm from identity theft and fraud, requiring them to take the time they would have dedicated to other life demands, to mitigate the actual and potential impact of the Data Breach.

135. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[12]

136. Other than offering twelve (12) months of credit monitoring and "identify theft restoration services," Defendant did not take any measures to assist Plaintiff and Class Members.

137. The limited offer of credit monitoring and the "identity theft restoration services" is woefully inadequate. While some harm has already taken place, the worst may be yet to come, as there could be a lag between when harm occurs and when it is discovered, and between when PII is acquired and when it is unlawfully used. Furthermore, identity theft monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's personally identifiable information). It does not prevent identity theft.[13]

138. Defendant's failure to adequately protect Plaintiff's and Class Members' PII has resulted in Plaintiff and Class Members having to undertake the above tasks, which require extensive amounts of time, correspondences, and for many of the credit and fraud protection services, payment of money. Plaintiff and Class Members have been charged with the foregoing responsibilities, all while Defendant does nothing of substance to assist them. Pursuant to Defendant's Notice Letter, TRISTAR placed the burden squarely upon Plaintiff and Class

---

[12] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[13] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

Members to discover possible fraudulent activity, identity theft, and mitigate the negative impacts arising from its Data Breach.

139. Plaintiff and Class Members have been damaged in several other ways as well. Plaintiff and Class Members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their PII. Plaintiff and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming task. Class Members have also been forced to purchase adequate credit reports, credit monitoring and other identity theft protection services, and have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity.

140. The PII stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen PII to send spear-phishing emails to Class Members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

141. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their PII;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost Opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to the PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate

measures to protect the PII in its possession;

- Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

- Anxiety and distress resulting from fear of misuse of the PII.

142. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their PII remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

143. Plaintiff brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a "Nationwide Class," and an "Oklahoma Subclass," (collectively defined as the "Class") defined as:

> **Nationwide Class**
> All persons whose personally identifiable information was submitted to Defendant and whose PII was compromised due to the Data Breach discovered in November 2022.
>
> **Oklahoma Subclass**
> All residents of Oklahoma whose personally identifiable information was submitted to Defendant and was compromised due to the Data Breach discovered in November 2022.

144. Excluded from the Classes are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

145. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

146. **Numerosity**—Federal Rule of Civil Procedure 23(a)(1). The members of the

Class are so numerous that joinder of all Class Members would be impracticable. On information and belief, the Class has thousands of members.

147. **Commonality and Predominance**—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable federal and state laws and regulations including, e.g., FTCA, and the applicable state data security regimes;

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant properly implemented their purported security measures to protect Plaintiff's and the Class's PII from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it initially became aware of its existence;

e. Whether Defendant disclosed Plaintiff's and the Class' personally identifiable information in violation of the understanding that the PII was being disclosed in confidence and should be maintained;

f. Whether Defendant's conduct constitutes breach of an implied contract;

g. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's PII;

h. Whether Defendant was negligent in failing to properly secure and protect

Plaintiff's and the Class's PII;

i. Whether Defendant was unjustly enriched by its actions; and

j. Whether Plaintiff and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

148. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on his own behalf, and that of the other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

149. **Typicality**—Federal Rule of Civil Procedure 23(a)(3). Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class Members were similarly injured through Defendant's uniform misconduct described above and were all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

150. **Adequacy of Representation**—Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate representative of the Class because his interests do not conflict with those of the Class he seeks to represent, he has retained counsel that is competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. Consequently, the Class' interests will be fairly and adequately protected by Plaintiff and his counsel.

151. **Injunctive Relief**—Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

152. **Superiority**—Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no

unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant. Thus, it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action mechanism presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class or, Alternatively, the State Subclass)

153. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

154. Upon Defendant's accepting and storing the PII of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the personally identifiable information was private and confidential and should be protected as such.

155. Defendant owed a duty of care not to subject Plaintiff's and Class Members' PII to an unreasonable risk of exposure and theft, as Plaintiff and Class Members were foreseeable and probable victims of any inadequate security practices.

156. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting,

and protecting PII in its possession;

- To protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

157. Defendant also breached its duty to Plaintiff and Class Members to adequately protect and safeguard PII by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, notwithstanding the known risk and foreseeable likelihood of breach and misuse that permitted a malicious third party to gather Plaintiff's and Class Members' personally identifiable information, and to potentially misuse it.

158. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew or should have known about numerous and recent well-publicized data breaches.

159. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

160. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

161. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

162. Because Defendant knew that a breach of its systems would damage thousands of its customers, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the personally identifiable information contained thereon.

163. Defendant's duty of care to use reasonable security measures arose from the special relationship that existed between Defendant and its customers, which is recognized by data privacy laws and regulations under the laws of thirteen (13) states.

164. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

165. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential personally identifiable information.

166. TRISTAR's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class Members' PII; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

167. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' personally identifiable information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class Members' PII;
- Failing to detect in a timely manner that Plaintiff's and Class Members' PII had been compromised; and
- Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

168. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, TRISTAR

unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PII within its possession or control.

169. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect Plaintiff's and the Class Members' PII and failing to provide them with timely notice that their sensitive information had been compromised.

170. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their personally identifiable information as described in this Complaint.

171. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class Members suffered damages as alleged above.

172. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the State Subclass)

173. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

174. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. When Plaintiff and Class Members submitted their respective insurance claims, they provided their personally identifiable information to Defendant.

175. In so doing, Plaintiff and Class Members entered implied contracts with Defendant whereby Defendant agreed to safeguard and protect such information and to timely detect any breach of their PII. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied

with relevant laws and regulations and were consistent with industry standards.

176. Plaintiffs and Class Members would not have entrusted their PII with Defendant in the absence of the implied contract between the parties.

177. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

178. TRISTAR breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII, and by failing to inform them of the Data Breach within a reasonable time.

179. As a direct and proximate result of Defendant's Breach of the implied contracts between Defendant, Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages (described in detail above).

180. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring (for a period to be determined by the Court) to all Class Members.

COUNT III
UNJUST ENRICHMEMT/QUASI-CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the Oklahoma Subclass)

181. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

182. As a third-party insurance administrator, TRISTAR derives monetary benefits from Plaintiff's and Class Members' personally identifiable information. In exchange, they should have been entitled to have Defendant protect their PII with adequate data security.

183. Defendant knew that Plaintiff and Class Members conferred a benefit on it and accepted and has retained that benefit. Notably, Defendant profited from Plaintiff's and Class Members PII and used their data for business purposes.

184. TRISTAR failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit the Plaintiff's and Class Members' personally

identifiable information provided.

185. Defendant acquired the PII through inequitable means as it failed to disclose the inadequate security practices previously alleged.

186. If Plaintiff and Class Members knew that TRISTAR would not secure their PII using adequate security, they would not have utilized Defendant's services, nor would they have entrusted Defendant with their personally identifiable information.

187. Plaintiff and Class Members have no adequate remedy at law.

188. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on it.

189. TRISTAR should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of the Nationwide Class or, Alternatively, the State Subclass)

190. Plaintiff and Class Members have an interest, both equitable and legal, in the PII that was conveyed to and collected, stored, and maintained by Defendant and which was ultimately compromised by unauthorized cybercriminals in the Data Breach.

191. Defendant, in taking possession of this highly sensitive information, has a special relationship with customers, including Plaintiff and the Class. As a result of that special relationship, Defendant was provided with and stored private and valuable information belonging to Plaintiff and the Class, which Defendant was required by law and industry standards to maintain in confidence.

192. Plaintiff and the Class provided personally identifiable information to Defendant under both the express and/or implied agreement of Defendant to limit and/or restrict completely the use and disclosure of such PII without Plaintiff's and Class Members' consent.

193. Defendant had a common law duty to maintain the confidentiality of Plaintiff's and Class Members' PII.

194. Defendant owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

195. As a result of the parties' relationship of trust, Defendant had possession and knowledge of the confidential personally identifiable information of Plaintiff and Class Members.

196. Plaintiff's and Class Members' PII is not generally known to the public and is confidential by nature. Moreover, Plaintiff and Class Members did not consent to, nor did they authorize Defendant to release or disclose their PII to unknown criminal actors.

197. Defendant breached the duty of confidence it owed to Plaintiff and Class Members when Plaintiff's and Class Members' PII was disclosed to unknown cybercriminals by way of Defendant's own acts and/or omissions, as alleged herein.

198. Defendant knowingly breached its duties of confidence by failing to safeguard Plaintiff's and Class Members' PII by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of costumer information that resulted in the unauthorized access and compromise of the personally identifiable information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to give adequate notice to Plaintiff and Class Members of the Data Breach; (g) failing to follow its own privacy policies and practices published to customers; (h) storing PII in an unencrypted and vulnerable manner, thereby allowing its disclosure to cybercriminals; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' PII to a criminal third party.

199. But for Defendant's wrongful breach of confidence owed to Plaintiff and Class

Members, their privacy would not have been compromised and their PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

200. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered or will suffer injuries, including but not limited to: loss of their privacy and confidentiality in their personally identifiable information; theft of their PII; costs associated with the detection and prevention of fraud and unauthorized use of their PII; costs associated with purchasing credit monitoring and identity theft protection services (including costs of the aforesaid services in excess of the twelve (12) months offered by Defendant); costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of Defendant's Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their personally identifiable information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and to not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the aforesaid data; and/or mental anguish accompanying the loss of confidence and disclosure of their confidential PII.

201. Defendant breached the confidence of Plaintiff and Class Members when it made an unauthorized release and disclosure of their confidential personally identifiable information and, accordingly, it would be inequitable for Defendant to retain any benefits it has received at Plaintiff's and Class Members' expense.

202. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal

damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT V
OKLAHOMA CONSUMER PROTECTION ACT
in Violation of Okla. Stat. tit. 15, § 751, et. seq.
(By Plaintiff Riggs on Behalf of the Oklahoma Subclass)

203. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

204. TRISTAR, Plaintiff and Oklahoma Class Members are "persons" as defined by Okla. Stat. tit. 15, § 752(1).

205. TRISTAR advertised, offered, or sold goods or services in Oklahoma and engaged in trade or commerce directly or indirectly affecting the people of Oklahoma, as defined by Okla. Stat. tit. 15, § 752(2).

206. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Okla. Stat. tit. 15, § §752(13)(14), including:

- Representing that its goods and services have characteristics, uses, and benefits that they do not have;
- Representing that its goods and services are of a particular standard or quality if they are of another;
- Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;
- Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is; and
- Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter.

207. TRISTAR's unfair, unconscionable, and deceptive practices include:

- Failing to implement and maintain reasonable security and privacy measures

to protect Plaintiff's and the Oklahoma Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Oklahoma Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Oklahoma Subclass Members' personally identifiable information, including the implementation and maintenance of reasonable security measures;
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Oklahoma Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Oklahoma's Subclass Members' PII; and
- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Oklahoma Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

208. TRISTAR's representations and omissions were material because they were likely to deceive reasonable customers about the adequacy of its data security and ability to protect the confidentiality of customers' personally identifiable information.

209. Defendant misled Plaintiff and Oklahoma Subclass Members to induce them to

rely on its misrepresentations and omissions.

210. Defendant acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff's and Oklahoma Subclass Members' rights.

211. As a direct and proximate result of TRISTAR's unfair, unconscionable, and deceptive practices, Plaintiff and Oklahoma Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; loss of the value of their PII; and the costs of identity protection services made necessary by the Data Breach.

212. Plaintiff and Oklahoma Subclass Members seek all monetary and non-monetary relief allowed by law, injunctive relief, and any other relief that is just and proper.

COUNT VI
INJUNCTIVE / DECLARATORY RELIEF
(On Behalf of the Nationwide Class)

213. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

214. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

215. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard users' PII and whether Defendant is maintaining data security measures adequate to protect the Class Members, including Plaintiff, from further data breaches that compromise their personally identifiable information.

216. Plaintiff alleges that Defendant's data-security measures remain inadequate. In

addition, Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their personally identifiable information and corresponding fraudulent activity will occur in the future.

217. Pursuant to the Court's authority under the Declaratory Judgment Act, Plaintiff asks the Court to enter a judgment declaring, among other things, the following: (i) Defendant owes a duty to secure customers' PII and to timely notify customers of a data breach under the common law and various federal and state statutes; and (ii) Defendant is in breach of these legal duties by failing to employ reasonable measures to secure customers' personally identifiable information in its possession and control and declining to inform them of the Data Breach.

218. Plaintiff further asks the Court to issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect customers' PII from future data Breach.

219. If an injunction is not issued, the Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event Defendant suffers a subsequent data breach. Further, the risk of another such breach is real, immediate, and substantial. If another breach of Defendant's networks and/or systems occurs, the Class Members will not have an adequate remedy at law because many of the resulting injuries would not be readily quantifiable and will therefore be forced to bring multiple lawsuits to rectify the same misconduct.

220. The hardship to the Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of Defendant, the Class Members will likely be subjected to substantial hacking and phishing attempts, fraud, and other misuse of their PII, in addition to the damages already suffered. Alternatively, the cost to Defendant of complying with an injunction by employing better and more reasonable prospective data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

221. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches of Defendant's networks and/or systems, thus eliminating the additional injuries to the Class

Members and the customers whose personal and confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an order certifying the proposed class and appointing Plaintiff and his counsel to represent the Class;

b. For an order awarding Plaintiff and Class Members actual, statutory, punitive, and/or any other form of damages provided by and pursuant to the statutes cited above;

c. For an order awarding Plaintiff and Class Members restitution, disgorgement and/or other equitable relief provided by and pursuant to the statutes cited above or as the Court deems proper;

d. For an order or orders requiring Defendant to adequately remediate the Data Breach and its effects;

e. For an order awarding Plaintiff and Class Members pre-judgment and post-judgment interest;

f. For an order awarding Plaintiff and Class Members treble damages, other enhanced damages and attorneys' fees as provided for under the statutes cited above and related statutes;

g. For an order awarding Plaintiff and the Class Members reasonable attorneys' fees and costs of suit, including expert witness fees;

h. For an order awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: February 23, 2024

By: */s/ Robert Mackey, Esq.*

Robert Mackey, Esq. (SBN 125961)
bobmackeyesq@aol.com
LAW OFFICES OF ROBERT MACKEY
660 Baker Street, Building A, Suite 201
Costa Mesa, CA 92626
Tel. (412) 370-9110

Nicholas A. Migliaccio (*pro hac vice* anticipated)
nmigliaccio@classlawdc.com
Jason S. Rathod (*pro hac vice* anticipated)
jrathod@classlawdc.com
MIGLIACCIO & RATHOD LLP
412 H Street NE, Suite 302
Washington, DC, 20002
Tel: (202) 470-3520
Interim Class Counsel for Plaintiff and the Proposed Class